Research Reports of the National Institute
of Industrial Safety, NIIS-RR-2004 (2005)
UDC 621.039.587:004.7:004.72.057.4:

安全制御用フィールドバスの基礎的安全要件とその考察*

齋藤　剛**，中村英夫***，三浦大樹****

An Inquiry into Basic Safety Requirements of Field-bus Network for Safety Control*

by Tsuyoshi SAITO**, Hideo NAKAMURA*** and Masaki MIURA****

***Abstract*:** In the bottom layer of a hierarchized computer network for manufacturing in a factory, serial communication networks, in which sensors, actuators and logic controllers are connected to a single wire (the bus) that has two endpoints, are collectively termed "Field Buses". Recently, application of the field bus technology to transmission of safety-related information from protective sensing devices for human safety to control parts of industrial machinery shows rapid progress. However, dangerous transmission errors on field buses and preventive measures against them have still not been investigated enough. The safety-related information transmission requires special considerations to ensure the promptness and inerrancy as well as the conventional hard-wired fail-safe interlock system.

This paper deals with the derivation of basic safety requirements of field bus network to transmit safety-related information (Safety Field Bus：SFB) and the experimental verification of safety performance of the SFB. From the perspective of the conventional fail-safe theories and requirements of international standards concerning safety of machinery, the four requirements are showed for the redundant architecture of processing interface controller, the cyclic signal transmission to confirm the normalcy of communication function and the double error detection coding of telegrams. In order to establish a concrete example of SFB system, a test model of safety control device capable of connected to SFB is experimentally produced by using a single board 16 bit microcomputer and a prepared SFB controller chip based on the controller area network (CAN) bus. Using the experimental SFB system including the test model, its response time to detect dummy hardware failures and to perform a designated safety function are measuared. From the results of the measurements, it is confirmed that the experimental SFB system has enough potential to achieve a higher safety integrity level than the level described on the associated international standards, however the importance of improvement in its slow response time was revealed.

***Keywords*;** Safety control, Field-bus network, Safety-related information, International standards, Dependable computing, Redundant diverse processor, Interface gate circuit

---

* 平成16年12月17日電気情報通信学会ディペンダブルコンピューティング研究会において，一部口頭発表した。
** 機械システム安全研究グループ Mechanical and System Safety Research Group
*** 日本大学理工学部 Nihon University, College of Science aud Technology
**** 春日電機㈱ Kasuga Electric Works Ltd.

1. はじめに

工場内の自動化機械や計測制御機器をデジタル通信回線で接続し，それらの情報をコンピュータで統合的に扱う階層的ネットワークのうち，最も下位に位置する階層，すなわち，生産現場に近いフィールド機器（センサ，アクチュエータ，操作機器）と制御装置（PLCやシーケンサ）との通信，または，これら制御装置同士の通信に特化したネットワークを“フィールドバス”と呼ぶ[1, 2]。従来，これらフィールド機器間での通信は，各信号を１対１関係で個々に接続して実現されてきたが，フィールドバスの導入によれば，１本の共用伝送路ケーブル（バスケーブル）で全情報の伝送が可能となる上，結線レイアウトも容易に変更できるようになる。このため，配線コストの削減，及び，据付け・保守整備時間の短縮を理由に急速に導入が進み[3]，現在，多くのプロトコルがオープン化されており，国際規格化されたものもある[4]。

この流れの中で，近年，製造ラインの各所に配置されたドアインタロックスイッチや光線式安全装置が出力する安全確認信号や緊急停止信号をフィールドバスにより伝送する技術が，欧州を中心に実用化されつつある[5, 6]。安全制御機器の通信にフィールドバス技術を導入すれば，省配線化・保守容易化のみならず，高機能な安全制御が実現可能となるが，そのためには，従来のハードロジックに基づく安全関連情報の伝送・制御で実現されていたのと同等以上のフェールセーフ性が確保されなければならず，安易な配線の置換が機械設備の誤動作による災害に直結する可能性もある。しかし，通信障害や伝送エラーの発生に対し，機械安全技術の視点から安全関連情報を扱うフィールドバス（以下，安全フィールドバスと呼ぶ）の危険側故障を考察した研究は少なく，緊急かつ重要な安全関連情報を確実に伝送するための技術的要件が明確に示されていないのが現状である。

本報では，これまでに開発・実用化されたフィールドバス技術の実態，ならびに，安全制御に関する既往の研究や国際安全規格の要求に基づき，危険側故障を回避するための安全フィールドバスの基礎的安全要件を明らかにする。さらに，CANバス（Control Area Network Bus[7]）をベースとする安全フィールドバスを利用してバス接続が可能な安全制御機器のモデルを試作し，上記要件の１つである故障検知時間に着目した実験結果から実現された安全性能を評価するとともに，内部信号処理部の冗長化構成について考察した結果を述べる。

2. フィールドバスの基本構造と利点

フィールドバスとは，センサ・アクチュエータ・各種スイッチといった検出端・操作端と，PLCやシーケンサ等の制御装置間の通信に特化した双方向シリアル通信ネットワークの総称である。インターネットや企業内LANといった，いわゆる情報系ネットワークとの相違点はそこで扱われる情報の内容にある。すなわち，情報系ネットワークでは，テキストメッセージ，画像・音声等のマルチメディア情報，計算機用プログラム等が伝送されるのに対し，フィールドバスでは，スイッチや電磁弁等のオンオフ信号，温度・圧力・速度等の計測データ，モータの速度制御指令といった計測制御情報が主な伝送対象となる。そのため，フィールドバスでは，一度に伝送すべき情報量は情報系ネットワークよりも少ないが，伝送要求があってから一定時間内に確実に通信処理を完了させるリアルタイム性が要求され，これに対する方策の違いが各種フィールドバスの特徴となっている。

以下では，汎用フィールドバスの具体的な例として，自動車産業分野を中心に広く普及しているCANバスの構造と動作を紹介するとともに，安全制御機器間の通信にフィールドバスを導入する利点について述べる。

2.1 CANバスの構造と動作

CANバスは，1980年代にBosch社が自動車内用分散型ネットワークとして開発したマルチマスター方式のシリアルバスであり，その後，1993年にISO規格化されたものである。**Fig. 1** に示すように，その接続形態は，120Ωの終端抵抗を有する２線式信号線の間の差動電圧を信号レベルとして検出するバス型トポロジであり，電磁的に厳しい環境においても良好なデータ通信を行える特長がある。実装された定性的エラー対策

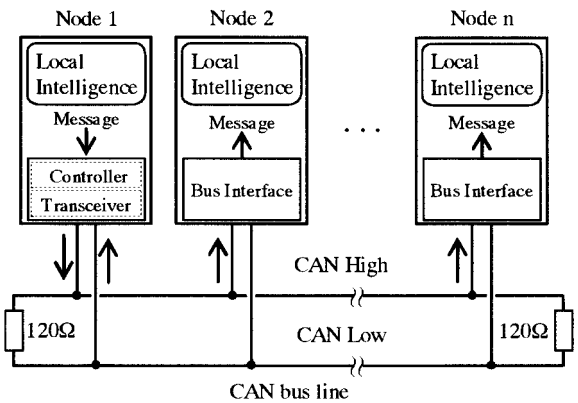

Fig. 1　Schematic diagram of CAN bus.
CANバスの基本ハードウェア構成

にも実績があり，このため，現在提案されている安全フィールドバスの多くが，CANバスをベースに開発されており，**Fig. 1** の接続形態を採用している。

バス上に接続機器（これをノードと呼ぶ）を増設する場合，ハードウェア的には，バスインターフェースを介してバスラインに機器を接続するだけでよく，省配線化と結線レイアウト変更の容易化が得られる。ここで，バスインターフェース（：Bus Interface Unit，以下，BIUと記す）とは，ノードの伝送情報（メッセージ）をCANバス専用のシリアル通信信号に変換するLSIユニットであり，メッセージのバッファ及び変換演算処理を行うコントローラと，通信信号の電気的調節を行うトランシーバから構成される。BIUによって変換されたメッセージは，バスライン上の電圧変化として全てのノードに同時に届き，同時に送信ノード自身（**Fig. 1** の例ではノード１）も変換された信号をチェックする。実際の通信状況の一例として，通信速度500 kbit/sの場合のCAN HighとCAN Lowの信号電圧，および，対応するビット値を**Fig. 2** に示す[8]。

制御パラメータ等のデータを送信する場合の通信信号の内部構成を**Fig. 3** に示す。CANバスはマルチマスター方式のバスで，その通信調停はCSMA/CA（Carrier Sense Multiple Access with Collision Avoidance）方式で行われる。すなわち，通信開始のタイミングが衝突しない場合は先に通信を開始したノードがバスを占有するが，２つ以上の通信がバス上で衝突した場合には，スタートビット（Start of Frame：SOF）に続く11ビットの識別子（Identifier）を双方が比較し，優先度の低いノードが送信を一時中止する。このため，識別子の送信時間だけで調停を完了でき，リアルタイム性の確保に適している。

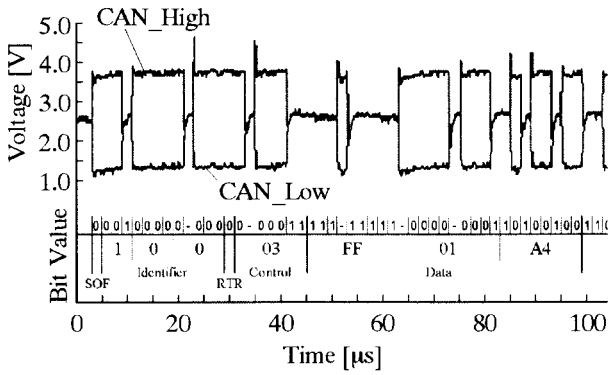

Fig. 2　An example of CAN bus comunication.[8]
CANバス通信の一例[8]

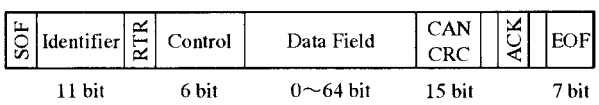

Fig. 3　Configuration of CAN standard data frame.
CANバスの通信信号の内部構造

一方，CAN CRC領域は，送信データの欠損や破壊を検定するための巡回冗長検査符号[9]（：Cyclic Redundancy Check Code，以下，CRCと記す）である。送信ノードと受信ノードでCRCを検査後，一致しない場合は通信障害の発生と見做し，エラーフレームが発信される。正常に受信が完了すれば，受信ノードは確認ビット（Acknowledgment：ACK）を直ちに上書きし，これを受けて，送信ノードは目的の機器への通信の完了を認識する。

2.2 安全制御機器へのフィールドバス導入の利点

一般に，安全制御機器は機械設備の各所に点在して配置され，また，それらの配線は冗長化されることが多い。このため，省配線化や保守容易化といったフィールドバスのメリットは，通常の制御システム以上に，安全制御を担う制御システムの安全関連部（以下，安全関連系と記す）でより発揮されるものと予想される。しかし，安全関連系にフィールドバスを導入することの真の意義は，以下で述べる優れた機能が実現可能となる点にある。すなわち，

1）デジタル信号化のみならず，前述したCRC等のソフトウェア的方策の利用や信号伝送媒体の適切な選択（例えば，フラットケーブルを光ファイバに換装すること）が可能となり，電磁ノイズ等の障害に対する耐性を著しく向上させることができる。
2）情報の多重化により，接続された機器からの危険検知信号と同時に，機器の正常性や劣化の情報も伝送でき，これらを統合的に扱えるようになる。
3）バス上の各機器はID等で明確に識別され，プログラム上で定義した仕様（コンフィグレーション）と常に照合される。このため，機器接続の変更や故意の無効化を常に監視できるようになる。また，定義したコンフィグレーションは，安全関連系の正確な構成図としてリスクアセスメント等に利用可能である。

しかし，これらのフィールドバス化の恩恵を得るには，ハードウェアの偶発的故障，ソフトウェアの決定論的障害，環境の影響といった様々な要因[10]で発生する伝送エラーに対し，安全関連系が危険側故障を生じないフェールセーフ性の立証が前提となる。

3. 安全フィールドバスの基礎的安全要件

安全制御に関する既往の研究では，フェールセーフな安全関連系は共通の制御論理構造を有することが明

らかになっており，これは安全情報伝達の原理と呼ばれる[11, 12]。安全フィールドバスが危険側故障の回避を保証するためには，少なくとも，その通信機能が安全情報伝達の原理に則して構成されなければならない。一方，現在，機械安全に関連した機器の安全要件や安全度水準は，ISO／IEC規格として国際的に統一されている。安全フィールドバスを直接扱う規格は今のところ存在しないが，関連する他の規格から要求されるであろう安全性能が類推できる。

これらの検討から，以下では，危険側故障の要因とそれに対する方策を整理し，安全フィールドバスがフェールセーフ性を有するための基礎的要件を明らかにする。

3.1 コントローラの冗長化構成

BIUのように，非対称誤り特性をもたない電子回路では，一般に，ある特定の入力に対する出力が期待した値（例えば参照値）と一致したことを逐次評価する方法でしか，演算機能の正常性を確認できない[13]。多数のメッセージを扱うBIUにおいて，全ての入力情報に対する参照値を予め記憶しておくことは非合理的であり，そのため，同程度の演算機能をもつ複数の処理系で同じ演算処理を行い，得られた結果を互いに比較することで，機能的に非対称誤り特性を実現することが基本となる。ここで，演算処理の冗長化には，実行時間をずらして処理を複数回繰りかえすソフトウェア的冗長化も考えられるが，単一障害に対する安全機能の維持[14]という理由から，ハードウェア的冗長化を選択するのが妥当である。

ただし，このハードウェア的冗長化は，BIUの核となるコントローラに課せられる要求であり，トランシーバとバスラインの冗長化は必ずしも必要はない。冗長化の極端な 2 つの例を**Fig. 4** に示す。ここで，**Fig. 4（a）**はBIU内部の各要素及びバスラインの全てを冗長化し，双方のコントローラ間でデータを交叉比較する構成，他方，**Fig. 4（b）**はコントローラのみを冗長化し，バスラインとトランシーバは単一系とした構成である。上述した**Fig. 4（a）**の構成で，特にコントローラの内部論理構造も完全に異なる場合には，偶発的な伝送エラーは 2 つの系で完全に独立であると見做せ，さらに決定論的障害も十分に抑制されるため，一般に高い安全性能が実現される。しかし，**Fig. 4（b）**の構成においても，後述する符号化や時間管理といった伝送エラーに対する方策をコントローラに組み込み，バスラインとトランシーバで起こる障害を全て危険側誤りと見做す構造をとれば，同等の安全性能を達成することが可能になる。この場合，バスラインとトランシーバには，危険側故障に対する安全性能ではなく，アベイラビリティ確保の意味での信頼性が要求される。

なお，コントローラの冗長化自体には，前述した内部論理構造が互いに異なるプロセッサを用いる異種冗長化[13]や，冗長化した処理系のバスデータをマシンサイクルレベルで常時照合するバス同期式[15]等の手法があるが，これについては第 5 章で詳述する。

3.2 通信機能の正常性確認

フェールセーフ性が立証可能な安全関連系では，すべての時刻tにおいて，次の論理的関係（安全情報伝達の原理）が成立しなければならない[11, 12]。

$$\forall t,\ S(t) \geqq S_c(t) \geqq E(t) \qquad (1)$$

ここで，$S(t) \in \{1, 0\}$は安全を表す論理変数，$S_c(t) \in \{1, 0\}$は安全確認のための検知手段の出力を表す論理変数，$E(t) \in \{1, 0\}$は機械の運転許可信号を表す論理変数であり，時刻tにおいて，各々，真に安全な状態にあるとき$S(t)=1$，検知手段が信号を出力しているとき$S_c(t)=1$，運転が許可されているとき$E(t)=1$とする。(1)式の論理不等号は，通報される安全$S(t)$の論理値とそれを伝達する信号$S_c(t)$，$E(t)$のエネルギの有無（信号のON／OFF）が一致することを要求

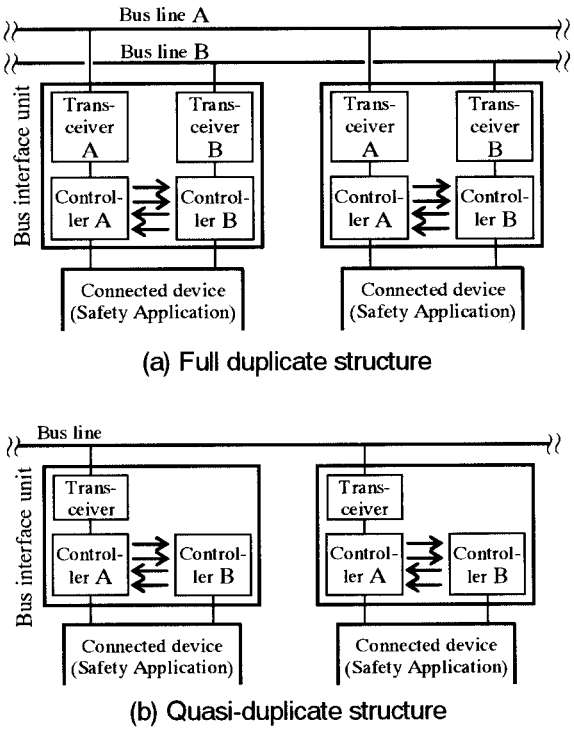

Fig. 4　Redundant structure of field-bus system for safety control.
安全フィールドバスの冗長化構造

している。これは，$S(t)=1$を示すON側信号を常時伝達することにより，同時に，安全関連系の情報伝達機能の正常性が確認されることを意味する。

安全フィールドバスにおいて，フェールセーフ性を立証するためには，少なくとも，その通信機能の論理構造が(1)式の関係を満たす必要がある。しかし，共通の伝送路に複数の機器が接続されているフィールドバスシステムでは，安全を示す情報を常に伝送して通信機能の正常性を検査することはできず，このため，一定周期毎に信号伝送を離散的に繰り返し，等価的に(1)式を満足することになる。

ここで，(1)式の時刻tがある一定の時間間隔Dと整数kによって(2)式の関係で離散化できるとすれば，(1)式を(3)式に書き換えることができる（ただし，$S(t)$は状態を示す変数であるので離散化されない)。

$$kD \leqq t < (k+1)D;\ k=0,1,\cdots \tag{2}$$

$$S(t) \geqq S_c[kD] \geqq E[kD] \tag{3}$$

(2)式の離散化は，いわゆる 0 次ホールドの変換であるので，(3)式が(1)式と等価である（すなわち，フィールドバス接続された安全関連系が安全情報伝達の原理を満たす）ためには，各変数間に次の関係が成立しなければならない。

$$\left.\begin{aligned} \forall t,\ S_c(t) &= S_c[kD] \\ E(t) &= E[kD] \end{aligned}\right\} \tag{4}$$

(4)式は，(3)式が(1)式と等価であるための十分条件であり，時刻tで$S(t)$ が 1 → 0 に変化したとき，$t=kD$でない限り$E[kD]=0$とはならず，時間間隔Dの分遅れて$E[(k+1)D]=0$となることが，安全確保上，許容できる場合に限り（機械システムの安全関連部の要求として，0 → 1 側の変化の遅れは一般に許容される)，(2)式の離散化が有効であることを意味している。このため，以下では，Dを検知遅れ時間と呼ぶことにする。

改めて，安全フィールドバスには，少なくとも $E\ [kD]$ が 1 → 0 に変化する側に関し，等価的に(1)式を満足すると見做せるほど，検知遅れ時間Dを小さくすることが要求される。当然，安全フィールドバスが適用される機械設備の状況により大きく異なるが，従来のハードロジックに基づく安全関連系と比較すれば，その許容時間は10～150 ms程度と見積もるのが妥当である。ただし，実際の検知遅れ時間Dは，単に正常性確認のための信号伝送周期のみでは決まらず，システムの演算処理サイクルや接続機器数といったシステムパラメータも影響する。この具体的な例については第 4 章で詳述する。

3.2 符号化による情報改ざんの検知

安全フィールドバスでは，従来の安全関連系と異なり，単に信号エネルギの有無だけで安全関連情報の健全性を評価することはできず，シリアル通信信号のビット列が伝送中に改ざんされていないことが受信時に確認できなければならない。このために有効な方策が，メッセージに付加される符号化処理である。**Fig. 3** に示したように，汎用のフィールドバスでも標準でCRC等の符号化処理を装備しており，送信器で変換・伝送されたメッセージが正確に受信・復調されたかを確認する。しかし，**Fig. 4(b)** に示したフィールドバスの構成では，バスラインとトランシーバで起こる伝送エラーを全て危険側誤りとして検知することが要求され，このため，冗長化されたコントローラで処理される安全関連情報用に特化した符号化処理が必要となる。

提案されているフィールドバスでは，受信器のアドレスと安全関連情報にCRC処理（メッセージの一連のビット列を多項式と見なし，これを別途定めた多項式で除算した剰余をメッセージに付加する操作[9])）を施し，通信信号内のデータ領域に安全関連情報用CRCを追加して格納する方法で，標準で装備されるCRCと 2 重化する例が多い。一例として，CANバスをベースとするSafety BUS pバス[5] の通信信号の内部構成を**Fig. 5** に示す。受信器アドレス，安全関連情報とともに16ビットの安全関連情報用CRCがデータ領域内にあり，これはCAN CRCとは独立して交叉比較機能付きの 2 重化コントローラで処理される。

2 つのCRCの符号長（付加される冗長化ビット数）は，メッセージの改ざんにより発生する危険側故障率が，安全性能として要求される危険側故障率の1/100以下となるように定められ[6]，標準で装備されたCRCと追加された安全関連情報用CRCは共に適切な多項式を選択したCRCであるとし，両者で発生する障害が独立事象と見做せるとすると，通信信号の改ざんによる危険側故障率$\Lambda\ [h^{-1}]$ は次式で与えられる[10]。

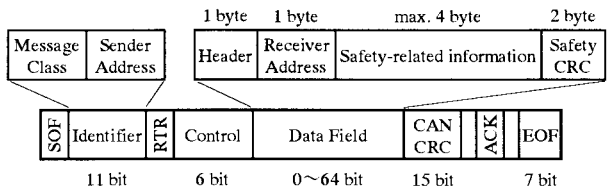

Fig. 5　Configuration of a data frame of Safety bus p protocol
Safety BUS p バスの通信信号の内部構造

$$\Lambda = 2^{-SC}\left(m \cdot n \cdot \lambda_{HW} + 2^{-BC} \cdot p \cdot v + \frac{1}{T_{cc}}\right) \quad (5)$$

ここで，SCは安全関連情報用CRCの符号長，BCは標準で装備されるCRCの符号長，λ_{HW}[h^{-1}] は単一系で構成されたバス伝送部の故障率，nは標準の符号化機構が異常を検知するまでの改ざんメッセージ数，mは安全率（通常は$m \geqq 5$），v[個／h] は単位時間あたりに伝送されるメッセージ数，pは使用している伝送媒体において電磁妨害等による1メッセージあたりのエラー発生頻度(一般的なフラットケーブルで約10^{-4}，光ファイバで約10^{-12})，また，T_{cc}［h］は改ざんメッセージが設定値を超え，冗長化コントローラがシステムを安全状態へ移行するまでの時間である。これらのパラメータは，BIUの冗長化構造やLSIの信頼性，使用する伝送媒体，導入されたエラー対策等，バスシステムのあらゆる条件に関連するため，一般化された要求としてSCとBCを定めることはできないが，例えば，**Fig. 5** に示したBC＝15，SC＝16の場合では$\Lambda < 10^{-9}$ [h^{-1}] が達成されている[6]。

3.4 情報処理理論に基づく伝送エラー防止方策

フィールドバス上で発生する伝送エラーは，次の7種類に大別できる。

1）反復：古いメッセージが繰り返し受信される，
2）欠損：メッセージが消去される，
3）挿入：別のメッセージが挿入される，
4）誤配列：メッセージの受信順序を誤る，
5）改ざん：メッセージの内容が書き換えられる，
6）遅延：規定の時間内に通信が完了しない，
7）偽装：認証されていない機器から信頼できない情報を受信する。

前節で述べた符号化は，5）改ざんに対する防止方策である。同様に他の伝送エラーに対しても，すでに多くの防止方策が情報処理技術の分野で確立されており[9, 16]，その有効性が実証されている。それらのうち，特に重要な方策を以下に示す。

1）送信元／受信先アドレスの同定：送信元／受信先アドレスをメッセージに含めることにより両者を同定し，登録されていない機器からの信用できない情報の挿入を阻止する。
2）タイムスタンプ：安全関連情報は一定時間内でのみ有効であり，古い安全の判断や確認を繰り返し発信してはならない。このため，送信器側でメッセージを生成した時刻をメッセージに付し，受信器側でその適時性を検査する。
3）シーケンス番号：送信された順序を示すシーケンス番号をメッセージに付し，バス上を伝送されたメッセージの前後関係を明らかにする。メッセージを受信した際に，その前のメッセージから分かる正しいシーケンス番号と照合する。
4）受信確認：受信器側から受信内容の逆送信，もしくは対応する確認メッセージの送信を行わせ，伝送が正しく行われたか送信器側で検査する。通常は，許容時間内に受信器側からの確認応答が得られない場合は，安全状態への移行処理が執られるタイムアウト機能を具備する。

伝送エラーと前述の符号化処理を含めた防止方策との対応関係を**Table 1** に示す。各伝送エラーに対して少なくとも1つの方策が施される必要がある。なお，以上の防止方策は，前述の交差比較機能付き冗長系の実行を前提としていることに注意が必要である。

3.5 接続される安全制御機器

改めて，安全フィールドバスがフェールセーフ性を有するための基礎的要件は，以下にまとめられる。

1）コントローラを交叉比較機能付き冗長化構成とし，機能的に非対称誤り特性を実現する。バスライン等の伝送部を単一系で構成する場合，そこで生じた伝送エラーは全て危険側誤りと見做す。
2）送受信器間で，伝送機能の正常性を確認するための信号伝送を周期的に繰り返し，故障を検知した場合には許容時間内に安全状態への移行処理を行うことで，等価的に(1)式を満足する。

Table 1　Relationship between transmission errors and preventive measures
伝送エラーと防止方策の関係

		Measures / Strategies				
		1) Identification Procedure	2) Time Stamp	3) Sequence Number	4) Acknowledge /Feedback	Safety Code
Transmission Error	1) Repetition		○	○		
	2) Deletion			○	○	
	3) Insertion	△		○	△	
	4) Resequence		○	○		
	5) Corruption				○	○
	6) Delay		○		○	
	7) Masquerade	○			△	○

○ : Effective
△ : Application dependant

3）メッセージの改ざんを検知するための安全関連情報用に特化した符号化機構を具備する。安全関連系と見做せない伝送部の機構とは独立させ，冗長化されたコントローラで処理する。
4）送信元同定機構やタイムスタンプ等の十分吟味された（Well-tried）伝送エラー防止方策を採用し，伝送情報の健全性・適時性を確保する。

ただし，これらの要件は，BIUのみならず，これに接続される安全制御機器にも適用される。例えば，BIUが正しく安全関連情報を受信できても，運転許可信号を扱う最終出力段がBIUと同等以上のフェールセーフ性を有する構造でなければ，単一故障を生じただけで機械を安全状態に移行することが不可能となる。要件 1）を完遂するためには，冗長化されたコントローラに各々独立した電源遮断手段を設け，どちらか一方の危険情報だけで機械を停止できるようにする必要がある。あるいは，接続機器が安全関連情報の生成を担う場合では，式(1)の安全情報伝達の原理に則した方法でBIUに情報を転送されなければならない。特に，3.2 節で述べたのと同様，BIUと機器側プロセッサとを接続する通信路では，その正常性を確認する目的で周期的な信号伝送が行われる必要がある。

4. フィールドバス接続が可能な安全制御機器の試作と検知遅れ時間の測定

提案されている安全フィールドバスのうち，前述したSafety BUS pバスを取り上げ，フィールドバス接続が可能な安全制御機器のモデルを試作した。Safety BUS pバスは，Pilz社の安全制御用シーケンスコントローラ[13]を上位管理デバイス（Management Device，以下，MDと記す）として使用するマルチマスター方式のネットワークであり，BIUのコントローラには異種冗長化構造が採用されている。

本章では，試作した安全制御機器モデルの構造を示すとともに，種々のシステムパラメータの条件で 3.2 節に述べた検知遅れ時間を測定し，得られた結果から実現された安全性能を考察する。

4.1 安全制御機器モデルの構造と基本動作

試作した安全制御機器モデル（以下，本モデルと記す）は，異種冗長化されたSafety BUS pコントローラとCANトランシーバから成るBIUと，これとデータバスを介して通信するシングルボード16ビットマイクロコンピュータ（ルネサステクノロジ社製H8/3687F，以下，H8マイコンと記す）より構成される。本モデルの外観を**Photo 1** に，また，その内部ブロック図を**Fig. 6** に示す。

安全関連情報の伝送は以下のように実現される。CANバスライン上を送信されたメッセージは，BIUのCANトランシーバに達し，さらに，コントローラAに転送される。コントローラAには，標準のCANコントローラが内蔵されており，これによりCAN CRCをデコードしてデータ領域の情報を読み込む（ここまでの処理は標準のCANバスと同じである）。読み込まれた情報は，コントローラAからコントローラBに転送され，両者でSafety BUS p CRCが処理されて，安全関連情報が抽出される。両者は，その結果を互いに転送して比較し，一致していれば本来の有効な情報として，これを接続されている安全制御機器のH8マイコンに転送する。

本モデルでは，あくまでバス接続を機能的に実現する目的で汎用のH8マイコンを利用しており，このため，両コントローラとの通信は単一系プロセッサで処理される。しかし，本来は，2 基のコントローラからの信号を個別に処理し，その内容を比較する交叉比較機能付き冗長系として構成される必要がある。このようなプロセッサの実際的な構成については，第 5 章で詳述する。

メッセージ送信は，これと逆の手順で行われ，接続機器からの情報を 2 基のコントローラで符号化し，変換結果が一致すれば，CANトランシーバを介して送信される。

H8マイコンが行うタスクは，大きく 2 つに大別できる。1 つは，バス全体を管理するMDとの通信であり，ログイン要求，デバイスIDの送信（このIDはMD内に保存されているコンフィグレーションの内容と照合される），初期データの転送，ならびに，これらの返答に対する受信確認である。Safety BUS pコントローラ内のメッセージバッファは常に監視されており，上記のような基本的な制御機能に関連する通信におい

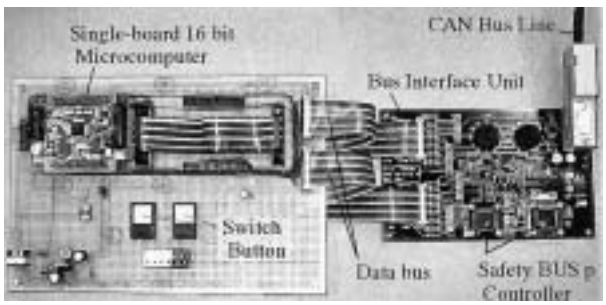

Photo. 1 Test model of a safety control device capable of connecting to Safety BUS p.
Safety BUS p バスに接続可能な安全制御機器の試作モデル

ても，到着メッセージが事前に設定した時間内に読み込まれない場合には機器全体がリセットされる。

もう１つのタスクは，Safety BUS pコントローラとの周期的な信号伝送であり，両者を接続するデータバスの結線と両者のI／Oポート動作の正常性を確認するためのものである。この信号伝送（以下，データバスチェックと記す）は4.5節で述べた要求に応えるもので，具体的には，一周期毎に全てのポートが少なくとも一度は論理値１と０のビットを送受信する（すなわち，ONとOFFの状態を繰り返す）よう構成された一連のデータパターンを伝送する。データバスチェックの一例を**Fig. 7** に示す。コントローラAとBのアドレス02h，03h番地に，８ビットデータ55h，AAhが書き込まれており，データラインを１本おきにチェックしているのが分かる。また，コントローラAのデータとコントローラBのデータとは互いにビット反転された関係にあり，両者の内部論理構造の相異も示されている。無音状態が一定時間続いた場合，BIUに対して上記の処理が実行されないと，コントローラ内のタイマにより機器全体がリセットされる。

なお，同様にCANバスラインの断線を検査する周期的信号伝送（以下，バスラインチェックと記す）が，MD側の制御を主体に実行される。バスラインチェックは，3.2節の要求に応えるもので，事前に設定した許容時間内に受信確認がない場合，これを故障と見做して安全状態への移行処理が行われる。

4.2 チェック周期と検知遅れ時間の関係

本モデルにおいて，データバスチェック及びバスラインチェックの各周期と検知遅れ時間Dとの関係は以下のように考えられる。

バスラインチェックにおいて，正常な通信が実行された後，発生したCANバスラインの故障を検出できるのは，次の通信に対して設定した許容遅れ時間を越えても受信確認がなされない時である。このため，バスラインチェックの周期をT_{bus}，受信確認の許容遅れ時間をT_{delay}で表すと，最悪の場合，故障検知までに$T_{bus}+T_{delay}$の時間を要することになる。他方，MDでは，バスラインチェックと非同期に，一定の演算処理サイクルに基づいて制御プログラムが実行されており，この中で，故障検知の通報を受けとる段階と安全状態への移行処理を行う段階は一度しかない。このため，MDのサイクル時間をT_{cycle}で表すと，安全状態への移行が実行されるまでに，最悪の場合，２回分のサイクル時間$2T_{cycle}$だけ遅れる可能性がある。以上の事を考慮すると，CANバスラインでの故障に対する検知遅れ時間D_{CAN}の最悪値は次式で与えられる。

$$D_{CAN} \leqq 2T_{cycle} + T_{bus} + T_{delay} \qquad (6)$$

一方，データバスの故障が検知された場合，Safety BUS pコントローラは接続機器側プロセッサを停止させるとともに，CANバス接続を一旦切断する。本モデルでは，MDはこの切断で接続機器内のデータバス故障を認識し，安全状態への移行処理を行う。したがって，データバスチェックの周期をT_{data}で表すと，データバスでの故障に対する検知遅れ時間D_{data}の最悪値は次式で与えられる。

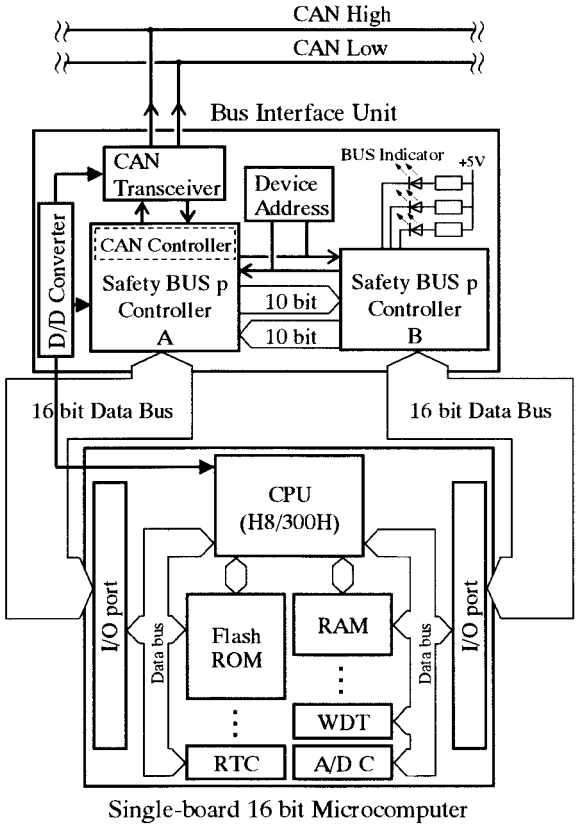

Fig. 6　Schematic block diagram of test model.
試作モデルの内部ブロック図

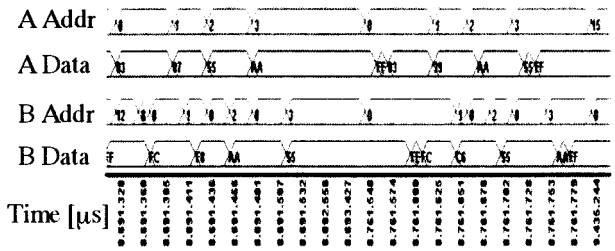

Fig. 7　An example of data transmission to confirm the normalcy of data buses and I/O ports.
データバス及びI／O ポートの正常性を確認するためのデータ伝送の一例

$$D_{data} \leqq T_{data} + 2T_{cycle} + T_{bus} + T_{delay} \qquad (7)$$

4.3 検知遅れ時間の測定と考察

以上を検証するため，本モデル内部にハードウェア故障を疑似的に起こし，MDがこれを検知し，システムを停止させるまでの時間を測定した。実験システムの構成を**Photo 2**に示す。ここでは，MDのI／Oモジュールに取り付けた汎用リレーユニット（オムロン㈱製MY4N）のOFF動作でシステムの停止を検出することとし，予備的実験から動作遅れ時間を予め同定しておき，測定された検知遅れ時間からその分を差し引いた。また，測定された検知遅れ時間は，疑似故障を起こすタイミングで大きくバラつく。そこで，各条件で10回の測定を行い，それらの平均値μと標準偏差σから$\mu+3\sigma$を求め，これを検知遅れ時間とした。

まず，CANバスラインのうち，CAN Lowをアナログスイッチを用いて電気的に切断する方法で疑似故障を発生させ，検知遅れ時間D_{CAN}の測定した。**Fig. 8**に，許容遅れ時間T_{delay}を20 msとし，バスラインチェック周期T_{bus}を20 ms，50 ms，100 msと変えたときのサイクル時間T_{cycle}に対する検知遅れ時間D_{CAN}の変化を示す。条件次第では約 6 倍もの違いが見られ，(6)式で示したように，各パラメータに強く影響されているのが分かる。ただし，(6)式で見積もられる値を超えることはなく，測定した範囲では，各パラメータと検知遅れ時間D_{CAN}との関係は概ね次式で近似できる。

$$D_{CAN} \fallingdotseq T_{cycle} + T_{bus} + T_{delay} \qquad (8)$$

(8)式による近似値を**Fig. 8** に破線で示す。これより，本測定では，ほぼ全ての場合において 1 回の演算処理サイクル内で故障検知動作が完了したと推察できる。

次いで，データバスのうち，コントローラAの 8 ビットデータの最下位ビットをアナログスイッチICを用いてGNDに短絡させる方法で検知遅れ時間D_{data}を測定した。バスラインチェック周期T_{bus}と許容遅れ時間T_{delay}をともに20 msとし，データバスチェックの周期T_{data}を20 ms，50 ms，100 msと変えたときのサイクルタイムT_{cycle}に対する検知遅れ時間D_{data}を**Fig. 9** に示す。検知遅れ時間D_{data}は，(7)式に示したようにD_{CAN}と比べてさらに延長されたが，そこで見積もられた値を超えてはおらず，(8)式の結果を考慮すると，測定した範囲では概ね次式で近似できる。

$$D_{data} \fallingdotseq T_{data} + 1.15T_{cycle} + T_{bus} + T_{delay} \qquad (9)$$

(9)式による近似値を**Fig. 9** に破線で示す。サイクル時間T_{cycle}にかかる係数は，データバスチェック周期と演算処理サイクルの非同期性を表していると考えられるが，プログラム構成等のシステムの特定の条件との関係までは把握できていない。

(6)，(8)式と(7)，(9)式の比較から，測定されたD_{data}は，CANバスの故障に対するD_{CAN}をも内包した，本モデルにおける実行上の通信機能の検査周期と見做すことができる。この場合，通信機能を担うフィールドバス系の平均故障率Pm［h^{-1}］は，構成ハードウェアの故障率をλ［h^{-1}］で表すと，$\lambda \cdot D_{data} \ll 1$の仮定の下では，次式で与えられる[13]。

$$Pm = \frac{\lambda}{2} D_{data} \qquad (10)$$

ただし，D_{data}の単位は時間（hour）とする。本測定

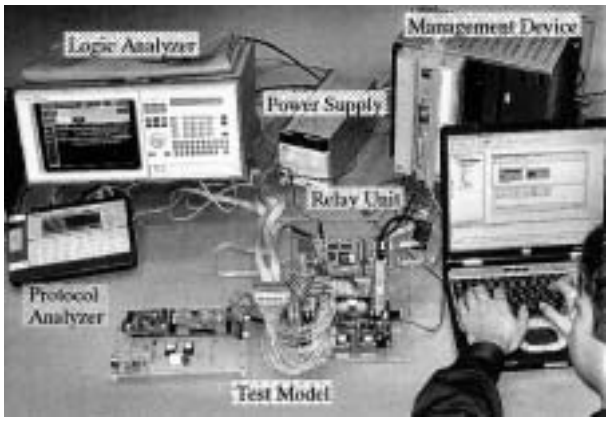

Photo. 2　Experimental setup to measure the response time to detect dummy failures.
擬似故障検知の応答時間を測定するための実験システム

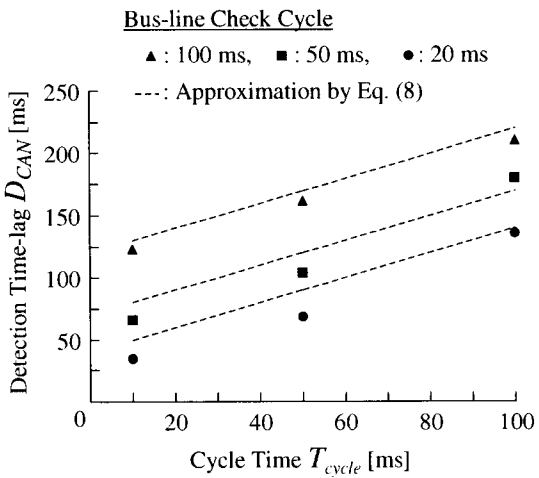

Fig. 8　Measurement result of the detection time-lag in case of CAN bus-line failure.
CANバスラインの故障に対する検知遅れ時間の測定結果

で用いた実験システムが高リスクに対応した安全関連部として運用されると仮定した場合，少なくとも，平均故障率Pm[h^{-1}] を10^{-9}[h^{-1}] 以下とすることが要求されると考えられる[6, 17]。そこで，本測定で得られた代表的な測定値として$D_{data}=5.56\times10^{-5}$h(200 ms) を(10)式に代入すると$\lambda<3.6\times10^{-5}$[h^{-1}] となる。これは，構成ハードウェアの平均故障間隔を約28000時間とすることに相当するが，現在のLSI機器製造の技術的水準から見れば，特に困難な要求ではない。

しかし，ここで行った測定は，本モデルだけが接続されたシステム構成で，他に負荷のかかるタスクもない比較的高速応答が期待できる条件下のものであったが，得られた結果は機械安全の分野で安全関連系に一般的に要求される応答性（10〜150 ms）と比べて必ずしも十分とは呼べないものであった。このため，安全フィールドバスが広く現場で使用されるには，今後より高速化を達成することが必要であると言える。

5. 接続機器側プロセッサの冗長化構造

本研究で試作したモデルは，あくまでバス接続を機能的に実現する目的で，汎用のシングルボードマイクロコンピュータを流用して構築しており，特に安全性能に配慮した構造は採用されていない。現実には，BIUに接続される機器側プロセッサは，第 4 章の基礎的安全要件に則し，両コントローラからの安全関連情報を別々に受信し，その健全性を交叉比較する 2 重系として構成されなければならない。

本章では，既往の冗長化プロセッサの構成法の比較に基づいて，高い安全性能を実現できるより実際的な機器側プロセッサの構造を提案するとともに，要因解析図に基づく故障分析から，その妥当性を検証する。

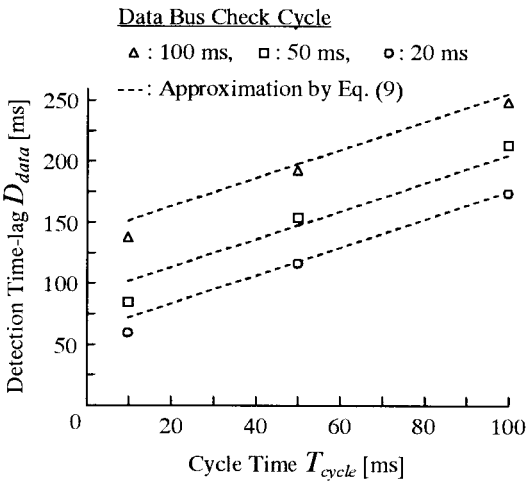

Fig. 9　Measurement result of the detection time-lag in case of data bus line failure.
データバスラインの故障に対する検知遅れ時間の測定結果

5.1 冗長化プロセッサの構成法

代表的な交叉比較機能付き冗長処理系の構造として，2 つのプロセッサ（Micro Processing Unit，以下，MPUと記す）のバスデータを別途設けたフェールセーフな照合回路によりマシンサイクルレベルで常時照合するバス同期式が知られている[13]。この構造は，現在，主に鉄道信号分野で採用されており，照合処理がハードウェアにより実行されることから，安全性能維持のために演算処理能力を低下させず，ソフトウェア開発も比較的簡単であるという利点がある。ただし，バスデータの比較を行うことから，2 つのMPUの論理構造やデータ構造が完全に一致していることが条件となり，このため，BIUからの通信データが両系で異なる場合，機器側MPUとしての採用は困難になる。

これに対し，前述した異種 2 重系構造は，内部論理構造，使用言語，クロック周波数等の諸仕様が互いに異なるMPUを 2 重化した構造である。ハードウェアの偶発的故障ばかりでなく，ソフトウェアバグやLSI製造過程での不具合といった決定論的障害も十分抑制できる特長があり，現在，主に欧州の製造設備で用いられている安全制御用プログラマブルコントローラの多くに異種冗長系が採用されている。

ただし，異種 2 重化MPUでの演算結果の照合では，バスレベルでの照合は行なえず，プログラムのチェックポイント毎での照合になる。このような照合の方法は，一般に，チェックポイント同期照合方式とチェックポイントデータ照合方式の 2 つに大別される。前者の同期照合方式は，プログラム上に設けたチェックポイントで同期を取る方式であり，照合成立を次のモジュールの開始条件とする場合が多い。このため，相互処理の時間差の総和分だけ処理速度が低下する。一方，後者のデータ照合方式では，例えば，相互の比較データをFIFOメモリに掃き出し，出力タイミングと非同期に照合を行うといった別のハードウェアで照合を実行する方法が採用でき，同期をとる必要がなくなる。しかし，この場合には，照合回路のフェールセーフ性に対する立証が別途必要となってくる。

5.2 機器側MPUの構成と故障分析

以上のことを考慮し，本研究では，接続機器側MPUの実際的な冗長化構造として，**Fig.10**に示す，異種冗長化された 2 つのMPUがチェックポイントでデータをデュアルポートメモリに書き込み，最終データの書き

込み信号を他系への割込み信号とするチェックポイント同期方式を提案する[18]。この構造では，両系の照合がミドルウェアで実施されるとし，相互の出力データとモジュール番号がチェックポイント毎に比較され，不一致時には安全状態への移行を実行する。このため，高安全性能の達成は，ミドルウェアを介した相互の照合とミドルウェアによる自己診断に委ねられる。

提案する冗長化構造の妥当性を，危険状態をトップイベントとする要因解析図を作成して検証した。その一部として，安全フィールドバスを介して非常停止指令を受信したときに，この指令を無視する事象をトップイベントとする要因解析図を**Fig.11**に示す。例えば，各モジュールの誤りに対しては，抑止ゲートとしてA，B両系で全く同一の誤りが同モジュールで発生することが条件となり，危険側故障へ至るパスは異種冗長化構造の採用によって分断される。また，冗長化されたコントローラが各々独立した電源遮断手段を有し，さらに，これら手段の動作が周期的に確認されて故障の蓄積が排除される構成では，不正に運転許可信号を出力する単一誤りは起こり得ない。以上の検討の結果，提案する構造は，ハードウェアの偶発的故障や電磁障害等による一過性誤り，ソフトウェアの決定論的障害に対し，十分な耐性を有することが確認された。

6. おわりに

伝送エラーの発生に対し，安全関連系が危険側故障を生じないことが立証されない限り，従来の配線を単純にフィールドバスで代用することはできない。そのための基礎的安全要件として，本報では，以下の４項目を挙げ，その方策について検討した。

1）交叉比較機能付き冗長化コントローラの採用，
2）伝送機能の正常性確認のための周期的信号伝送，
3）安全関連情報用に特化した符号化機構の具備，
4）Well-triedな情報処理理論的方策の採用。

さらに，安全フィールドバスに接続された安全制御機器の具体例として，Safety BUS pコントローラと汎用マイクロコンピュータを用いたモデルを試作し，故障検知時間に着目した動作確認実験を行った。その結果，現行の国際安全規格で要求されるレベルの安全性能は達成可能であるものの，さらに応答性の向上が必要となることを指摘した。また，試作したモデルは，あくまでバス接続を機能的に実現する目的で構築しており，機器側プロセッサには安全性能に配慮した構造は採用されていない。このため，より実際的な構造として，チェックポイント同期方式冗長化構造を提案し，要因解析図に基づく故障分析から，その妥当性を確認した。

フィールドバス接続された安全関連系は，デジタル通信システムとして著しく高い拡張性を備えるが，本研究での検討は，限られた構成のシステムまでしか及んでいない。今後より多くの事例を踏まえ，さらに議論を深めたい。

謝　辞

本研究は，春日電機株式会社との共同研究として実施されたものであり，特に機器試作及びその動作解析において関係諸氏に多大なご協力をいただいた。また，日本大学理工学部電子情報工学科の内藤正偉氏には，交叉比較機能付き冗長処理系の故障解析に大変尽力いただいた。以上を記して，ここに謝意を表す。

参考文献

1）Andy McFarlane： Fieldbus Review, Sensor Review, Vol.17，No.3（1997）pp.204-210.
2）深川真輝：フィールドバス，産総研ニュース，Vol.3, No.3（1997）.
3）特集「フィールドバスの将来」，計測技術，Vol.30, No.10（2002）pp.1-29.
4）Richard Piggin, Ken Young, Richard McLaughlin: The current fieldbus standards situation. A European view, Assmbly Automation, Vol.19, No.4（1999）pp.286-289.
5）Richard Piggin：A fieldbus for machine safety, IEE Review, Vol.46, No.4（2000）pp.33-37.
6）Reinert D., Schaefer M.（田中紘一監訳）：オートメーション用安全バスシステム，NPO安全工学

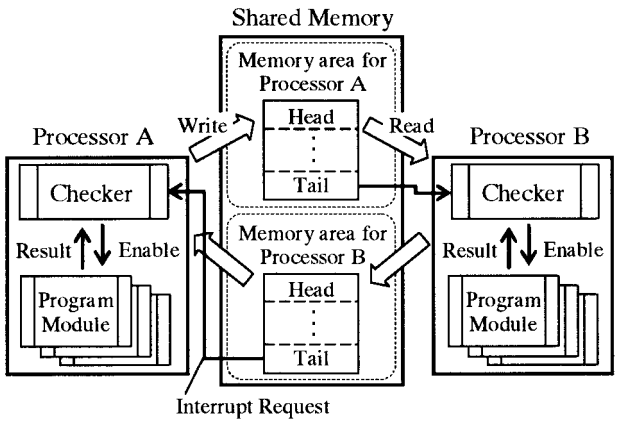

Fig. 10　An redundant diverse architecture of micro processing unit instakked in a device connected to safety-related field bus.
安全フィールドバスに接続される機器の異種冗長化MPUの構造

研究所（2003）.
7）ISO 11898, Road vehicles - Interchange of digital information - Controller area network（CAN）for high-speed communication（1993）.
8）ベクター・ジャパン株式会社ホームページ，www.vector-japan.co.jp/products/can_details.html.
9）今井秀樹：符号理論，電気情報通信学会編，コロナ社（1990）.
10）IEC 62280, Railway applications-Communication, signaling and processing systems-Part 2：Safety-related communication in open transmission systems（2002）.
11）杉本旭，蓬原弘一：安全の原理，機論C，Vol.56，No.530（1990）pp. 2601-2609.
12）杉本旭，蓬原弘一：安全制御系における安全情報のエネルギー伝達，機論C，Vol.56，No.530（1990）pp. 2658-2665.
13）齋藤剛，池田博康，杉本旭：非対称誤り特性を有するガス検知システムの基礎的要件と構成法，産業安全研究所特別研究報告，NIIS-SRR-No.27（2002）pp.63-76.
14）ISO 13849, Safety of machinery：Safety-related parts of control systems（1999）.
15）中村英夫，武子淳：次世代運転制御システム

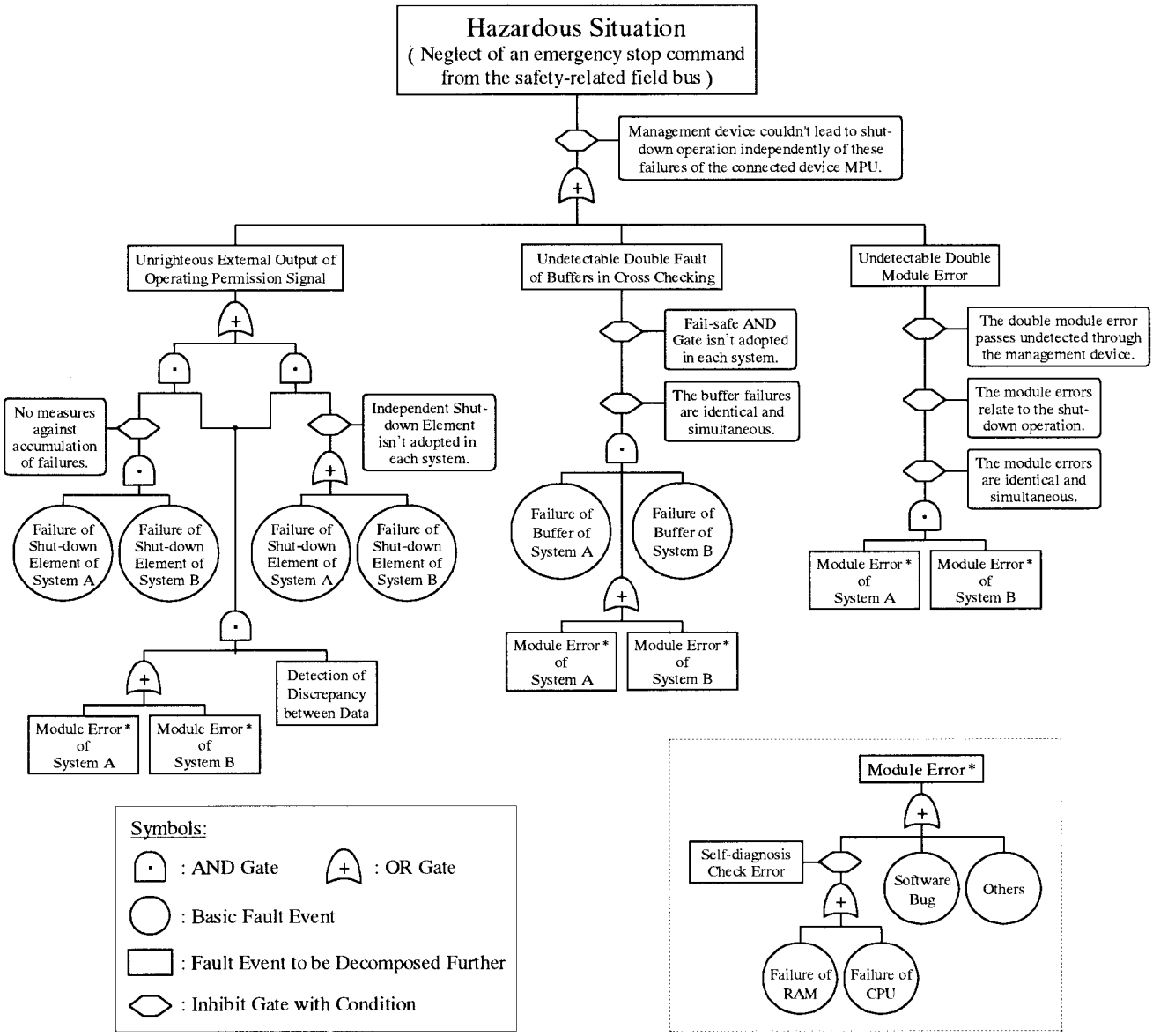

Fig. 11　An example of factorial analysis for verification of proposed rebundant diverse MPU.
(in case that it is assumed as the top event that the device neglects an emergency stop command)
提案する異種冗長化MPUの要因解析図の一例（非常停止指令の無視をトップイベントとした場合）

CARAT用マルチプロセッサシステムのディペンダブル設計，電学論D，Vol.114，No.5（1994）pp.499-504.
16）当麻善弘：フォールトトレランスシステム論，電気情報通信学会編，コロナ社（1990）.
17）IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems（1998）.
18）内藤正偉，望月寛，中村英夫，齋藤剛：産業用セーフティバスとインターフェースの検討，信学技報，DC-2004-87（2004）pp.25-32.

（平成17年 1 月11日受理）